Apellidos: ..... Grupo: .....

Nombre: ..... nif: .....

ALEM

Grado en Ingeniería Informática

7 de noviembre 2017

1. Responde brevemente las siguientes cuestiones:

   a) Sea x el número cuya representación en complemento a 2 es 110101101010. ¿Qué número es x?

   b) ¿Cuántos divisores positivos tienen los números: 1800, $5^3 \cdot 6^2 \cdot 8^4$, 11!?

   c) ¿Cuántas unidades hay en $\mathbb{Z}_{117}$?

   d) ¿Es cierto que $4^{36} = 1$ en $\mathbb{Z}_{73}$?

   Solución:

   a) Vemos en primer lugar que el número x es negativo, pues su primera cifra es 1. Tenemos entonces dos formas de calcular x:

   - Escribimos $-x$ en complemento a 2, en cuyo caso tendremos la representación binaria de $-x$, y a partir de ahí obtenemos su expresión decimal:

     $$110101101010 \longrightarrow 001010010101 \longrightarrow 001010010110$$

     Y ahora vemos que $-x = 2^9 + 2^7 + 2^4 + 2^2 + 2 = 512 + 128 + 16 + 4 + 2 = 662$, luego $x = -662$.
   - Pasando directamente a decimal:

     $$x = -2^{11} + 2^{10} + 2^8 + 2^6 + 2^5 + 2^3 + 2 = -2048 + 1024 + 256 + 64 + 32 + 8 + 2 = -662.$$

     Notemos que al tener la última cifra repetida podemos quitarla, con lo que la expresión en complemento a 2 de x podría ser también 10101101010, y al pasarla a decimal nos quedaría $-1024 + 256 + 64 + 32 + 8 + 2 = -662$.

   b) Factorizamos cada uno de los números como producto de primos, y a partir de ahí obtenemos el número de divisores:

   - $1800 = 2^3 \cdot 3^2 \cdot 5^2$. El número de divisores positivos es $(3+1)(2+1)(2+1) = 36$.
   - $5^3 \cdot 6^2 \cdot 8^4 = 5^3 \cdot (2 \cdot 3)^2 \cdot (2^3)^4 = 5^3 \cdot 2^2 \cdot 3^2 \cdot 2^{12} = 2^{14} \cdot 3^2 \cdot 5^3$, que tiene $15 \cdot 3 \cdot 4 = 180$ divisores.
   - $11! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$, que tiene $9 \cdot 5 \cdot 3 \cdot 2 \cdot 2 = 540$ divisores.

   c) El número de unidades de $\mathbb{Z}_{117}$ es $\varphi(117)$. Como $117 = 3^2 \cdot 13$, $\varphi(117) = \varphi(3^2) \cdot \varphi(13) = (3^2 - 3)(13 - 1) = 6 \cdot 12 = 72$.

   d) Tenemos que $4^{36} = (2^2)^{36} = 2^{72}$. Al ser 73 un número primo, por el teorema de Fermat sabemos que $2^{73-1} = 2^{72} = 1$ en $\mathbb{Z}_{73}$. La respuesta es entonces que sí.

2. Calcula todas las soluciones positivas menores que 20000 del sistema de congruencias

$$\begin{array}{rcrcr} 45x & \equiv & 59 & \text{mód} & 77 \\ 29x & \equiv & 43 & \text{mód} & 70 \\ 33x & \equiv & 27 & \text{mód} & 78 \end{array}$$

Solución:

En primer lugar resolvemos el sistema de congruencias:

$45x \equiv 59$ mód 77
$45 \cdot 12x \equiv 59 \cdot 12$ mód 77
$x \equiv 708$ mód 77
$x \equiv 15$ mód 77
$x = 15 + 77k$

$29x \equiv 43$ mód 70
$29(15 + 77k) \equiv 43$ mód 70
$435 + 2233k \equiv 43$ mód 70
$15 + 63k \equiv 43$ mód 70
$63k \equiv 28$ mód 70
$9k \equiv 4$ mód 10
$9 \cdot 9k \equiv 4 \cdot 9$ mód 10
$k \equiv 6$ mód 10
$k = 6 + 10k'$
$x = 15 + 77(6 + 10k')$
$x = 477 + 770k'$

$33x \equiv 27$ mód 78
$33(477 + 770k') \equiv 27$ mód 78
$15741 + 25410k' \equiv 27$ mód 78
$63 + 60k' \equiv 27$ mód 78
$60k' \equiv -36$ mód 78
$60k' \equiv 42$ mód 78
$10k' \equiv 7$ mód 13
$10 \cdot 4k' \equiv 7 \cdot 4$ mód 13
$k' \equiv 2$ mód 13
$k' = 2 + 13k''$
$x = 477 + 770(2 + 13k'')$
$x = 2017 + 10010k''$

A continuación detallamos algunos de los cálculos realizados:

- Puesto que $\text{mcd}(45, 77) = 1$ la congruencia $45x \equiv 59$ mód 77 tiene solución.
- Necesitamos el inverso de 45 módulo 77.

77		0
45		1
32	1	v_1
13	1	v_2
6	2	v_3
1	2	v_4

$v_1 = 0 - 1 \cdot 1 = -1$
$v_2 = 1 - 1 \cdot (-1) = 2$
$v_3 = -1 - 2 \cdot 2 = -5$
$v_4 = 2 - 2 \cdot (-5) = 12$

77		0
45		1
32	1	-1
13	1	2
6	2	-5
1	2	12

Luego $45^{-1} = 12$

- $\text{mcd}(63, 70) = 7$, y 28 es múltiplo de 7. Por tanto, la congruencia $63k \equiv 28$ mód 70 tiene solución, y para resolverla se divide todo por 7.
- El inverso de 9 módulo 10 vale 1.
- $\text{mcd}(60, 78) = 6$. Puesto que 42 es múltiplo de 6, la congruencia $60k' \equiv 42$ mód 78 tiene solución.
- Calculamos 10^{-1} módulo 13.

13		0
10		1
3	1	v_1
1	3	v_2

$v_1 = 0 - 1 \cdot 1 = -1$
$v_2 = 1 - 3 \cdot (-1) = 4$

13		0
10		1
3	1	-1
1	3	4

Luego $10^{-1} = 4$

La solución del sistema de congruencias es $x = 2017 + 10010k'$. Como buscamos soluciones entre 0 y 20000, acotamos los valores de k''.

$$\begin{array}{ccccc} 0 & \leq & x & \leq & 20000 \\ 0 & \leq & 2017 + 10010k'' & \leq & 20000 \\ -2017 & \leq & 10010k'' & \leq & 17983 \\ \frac{-2017}{10010} & \leq & k'' & \leq & \frac{17983}{10010} \\ -0'2 & \leq & k'' & \leq & 1'79 \\ 0 & \leq & k'' & \leq & 1 \end{array}$$

Es decir, $k'' = 0, 1$, lo que nos da las soluciones $x = 2017$ y $x = 12027$.

3. Sea $A = \mathbb{Z}_3[x]_{x^3+2x^2+x+1}$.

   a) ¿Cuántos elementos tiene A?

   b) ¿Es A un cuerpo?

   c) Encuentra, si es posible, un elemento $\alpha \in A$ tal que

$$(\alpha + x^2 + 1)(x^2 + x) = \alpha(2x^2 + 2x + 2).$$

Solución:

a) El número de elementos de A es $3^3 = 27$. Estos 27 elementos son:

0	x	$2x$	x^2	x^2+x	x^2+2x	$2x^2$	$2x^2+x$	$2x^2+2x$
1	$x+1$	$2x+1$	x^2+1	x^2+x+1	x^2+2x+1	$2x^2+1$	$2x^2+x+1$	$2x^2+2x+1$
2	$x+2$	$2x+2$	x^2+2	x^2+x+2	x^2+2x+2	$2x^2+2$	$2x^2+x+2$	$2x^2+2x+2$

b) Para que A sea un cuerpo, todos los elementos anteriores, salvo 0, deben tener inverso. Esto ocurre si el polinomio $m(x) = x^3 + 2x^2 + x + 1$ es irreducible.
Al ser $m(x)$ un polinomio de grado 3, para comprobar si es o no irreducible basta comprobar si tiene o no raíces. Tenemos que $m(0) = 1$, $m(1) = 5 = 2$, $m(2) = 19 = 1$. Vemos entonces que $m(x)$ no tiene raíces luego es irreducible. En tal caso, A es un cuerpo.

c) Tenemos que resolver una ecuación donde la incógnita es α. Vemos que esta ecuación es de grado 1. Despejamos entonces α.
$(\alpha + x^2 + 1)(x^2 + x) = \alpha(2x^2 + 2x + 2)$.

$\alpha(x^2 + x) + (x^2 + 1)(x^2 + x) = \alpha(2x^2 + 2x + 2)$.

$\alpha(x^2 + x) - \alpha(2x^2 + 2x + 2) = -(x^2 + 1)(x^2 + x)$.

$\alpha(x^2 + x - 2x^2 - 2x - 2) = -(x^4 + x^3 + x^2 + x)$.

$\alpha(2x^2 + 2x + 1) = 2x^4 + 2x^3 + 2x^2 + 2x$.

$\alpha(2x^2 + 2x + 1) = x^2 + 2x + 2$.

$\alpha = (x^2 + 2x + 2) \cdot (2x^2 + 2x + 1)^{-1}$.
En un momento de estos cálculos hemos sustituido $2x^4 + 2x^3 + 2x^2 + 2x$ por $x^2 + 2x + 2$. Esto es así, ya que en A ambos elementos son iguales, como nos lo pone de manifiesto la siguiente división:

	2	2	2	2	0
1		2	1	1	2
2			1	2	
2					
	2	1	1	2	2

Luego $2x^4 + 2x^3 + 2x^2 + 2x = (x^3 + 2x^2 + x + 1) \cdot (2x + 1) + x^2 + 2x + 2$

Calculamos ahora el inverso de $2x^2 + 2x + 1$.

División de $x^3 + 2x^2 + x + 1$ entre $2x^2 + 2x + 1$

2	1	2	1	1
2		2	1	1
1			2	
	1	1	1	2

$c_1(x) = 2 \cdot (x + 1) = 2x + 2$
$r_1(x) = x + 2$

División de $2x^2 + 2x + 1$ entre $x + 2$

	2	2	1
1		2	1
	2	1	2

$c_2(x) = 2x + 1$
$r_2(x) = 2$

Con estas divisiones, calculamos $(2x^2+2x+1)^{-1}$.

x^3+2x^2+x+1		0
$2x^2+2x+1$		1
$x+2$	$2x+2$	$x+1$
2	$2x+1$	x^2
1		$2x^2$

$0-1\cdot(2x+2)=x+1$
$1-(2x+1)\cdot(x+1)=1-(2x^2+1)=x^2$

Y ya tenemos que $(2x^2+2x+1)=2x^2$, luego $\alpha=(x^2+2x+2)\cdot 2x^2=2x^4+x^3+x^2=2x^2+x$. Este último resultado se obtiene de la división:

	2	1	1	0	0
1		2	1	1	0
2			0	0	
2					
	2	0	2	1	0

4. Sean $p(x) = x^5 + 2x^3 + x + 4$ y $q(x) = x^4 + 3x^2 + 2x + 2$ dos polinomios con coeficientes en $\mathbb{Z}_5$.

   a) Calcula $\mathrm{mcd}(p(x), q(x))$.

   b) Factoriza $p(x)$ como producto de irreducibles.

   Solución:

   a) Para calcular el máximo común divisor de los dos polinomios nos valemos del algoritmo de Euclides. Realizamos las correspondientes divisiones:

$p_1(x) = x^5 + 2x^3 + x + 4$

$q_1(x) = x^4 + 3x^2 + 2x + 2$

	1	0	2	0	1	4
0		0	2	3	3	0
2			0	0	0	
3						
3						
	1	0	4	3	4	4

$c_1(x) = x$

$r_1(x) = 4x^3 + 3x^2 + 4x + 4$

$p_2(x) = x^4 + 3x^2 + 2x + 2$

$q_2(x) = 4x^3 + 3x^2 + 4x + 4$

4	1	0	3	2	2
2		3	4	4	2
1			4	2	
1					
	4	2	1	3	4

$c_2(x) = 4x + 2$

$r_2(x) = x^2 + 3x + 4$

$p_3(x) = 4x^3 + 3x^2 + 4x + 4$

$q_2(x) = x^2 + 3x + 4$

	4	3	4	4
2		3	4	1
1			2	
	4	1	0	0

$c_3(x) = 4x + 1$

$r_3(x) = 0$

   Puesto que el último resto no nulo es $x^2 + 3x + 4$, y éste es un polinomio mónico tenemos que $\mathrm{mcd}(p(x), q(x)) = x^2 + 3x + 4$.

   b) Para factorizar $p(x)$, y puesto que $x^2 + 3x + 4$ es un divisor suyo, dividimos $p(x)$ entre $x^2 + 3x + 4$.

	1	0	2	0	1	4
2		2	1	2	2	1
1			4	4	2	
	1	2	2	1	0	0

$$p(x) = (x^2 + 3x + 4) \cdot (x^3 + 2x^2 + 2x + 1)$$

   Y ahora factorizamos $p_1(x) = x^2 + 3x + 4$ y $p_2(x) = x^3 + 2x^2 + 2x + 1$. Puesto que son de grados 2 y 3 respectivamente, únicamente hemos ver si tienen o no raíces.

   - $p_1(0) = 4$, $p_1(1) = 8 = 3$, $p_1(2) = 14 = 4$, $p_1(3) = 22 = 2$, $p_1(4) = 32 = 2$. Vemos que $p_1(x)$ no tiene raíces, luego es irreducible.
   - $p_2(0) = 1$, $p_2(1) = 6 = 1$, $p_2(2) = 21 = 1$, $p_2(3) = 52 = 2$, $p_2(4) = 105 = 0$. Como 4 es raíz de $p_2(x)$, lo dividimos por $x - 4 = x + 1$.

	1	2	2	1
4		4	4	4
	1	1	1	0

     De donde $p_2(x) = (x + 1) \cdot (x^2 + x + 1)$. Este último polinomio podemos ver fácilmente que es irreducible (pues $x = 4$ no es raíz).

   Finalmente, tenemos la factorización de $p(x)$:

$$p(x) = (x + 1) \cdot (x^2 + x + 1) \cdot (x^2 + 3x + 4).$$